
RouteFinder[®]

Internet Security Appliance

RF850

RF860

Quick Start Guide



Quick Start Guide

RouteFinder RF850/860

82100051L, Revision B

Copyright

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 2006-7, by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Trademarks

Trademarks and Registered Trademarks of Multi-Tech Systems, Inc.: Multi-Tech, the Multi-Tech logo and RouteFinder. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. Kaspersky Anti-Virus engine is copyrighted by Kaspersky Labs. GNU General Public License is copyrighted by Free Software Foundation, Inc. Surfcontrol is the registered product of Surfcontrol PLC.

Record of Revisions

Revision	Date	Description
A	04/10/06	Initial release. Software version 3.30.
B	04/05/07	Changes for software version 3.32. Updated Technical Support contact list.

Patents for the RouteFinder and the Modem

The RouteFinder is covered by one or more of the following U.S. Patent Numbers: 6,219,708; 5,301,274; 5,309,562; 5,355,365; 5,355,653; 5,452,289; 5,453,986.

The modem is covered by one or more of the following U.S. Patent Numbers: 6,031,867; 6,012,113; 6,009,082; 5,905,794; 5,864,560; 5,815,567; 5,815,503; 5,812,534; 5,809,068; 5,790,532; 5,764,628; 5,764,627; 5,754,589; D394,250; 5,724,356; 5,673,268; 5,673,257; 5,644,594; 5,628,030; 5,619,508; 5,617,423; 5,600,649; 5,592,586; 5,577,041; 5,574,725; D374,222; 5,559,793; 5,546,448; 5,546,395; 5,535,204; 5,500,859; 5,471,470; 5,463,616; 5,453,986; 5,452,289; 5,450,425; D361,764; D355,658; D355,653; D353,598; D353,144; 5,355,365; 5,309,562; 5,301,274 Other Patents Pending.

Technical Support

Country	By Email	By Phone
France	support@multitech.fr	+(33) 1-64 61 09 81
Europe, Asia, Africa	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others	support@multitech.com	800-972-2439 or +763-785-3500

Warranty, Repairs & Service, Licenses

The following statements and policies are printed in the RouteFinder User Guide. They are also available on the RouteFinder CD.

- Multi-Tech Systems, Inc. Warranty Statement
- Multi-Tech Systems, Inc. Repairs and Service Policy
- Multi-Tech Systems, Inc End User License
- GNU General Public License
- SurfControl URL Filtering End-User Terms
- Kasperkey Standard End User License Agreement.

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Internet Address: <http://www.multitech.com>

Contents

Chapter 1 – Introduction	4
RouteFinder Documentation	4
Safety Warnings.....	4
Shutdown Caution	5
Ship Kit Contents.....	5
License Keys	5
Chapter 2 – Installation	6
Installation Notes	6
Front Panel	6
Cabling Procedure.....	7
Setting up a Workstation and Starting the RouteFinder.....	8
Open a Web Browser.....	10
Login	10
Web Management Software Opens.....	11
Navigating Through the Software Screens	11
Chapter 3 – Configuration Using Web Management Software	13
Initial Configuration Step	13
Second Configuration Step – Using the Wizard Setup.....	13
The Wizard Setup Screen.....	14
Chapter 4 – Configuration Examples	15
Example 1 – Setup Two RouteFinders	15
Example 2 – Set Up Two RouteFinders Behind a NAT Device.....	21
Example 3 – Remote Client-to-LAN Configuration Using DNAT and Aliasing	27
Example 4 – Client-to-LAN Configuration Using PPTP Tunneling	28
Checking the Tunnel	28
Chapter 5 – URL Categorization	29

Chapter 1 – Introduction

RouteFinder Documentation

This Quick Start Guide is intended to provide the experienced system administrator the information needed to quickly get the RouteFinder up and running. A User Guide with more detailed information is provided on the RouteFinder CD or the Multi-Tech Systems, Inc. Web site.

Safety Warnings

Lithium Battery Caution

Danger of explosion if battery is incorrectly replaced. A lithium battery on the RouteFinder PC board provides backup power for the time-keeping capability. The battery has an estimated life expectancy of ten years. When it starts to weaken, the date and time may be incorrect. If the battery fails, send the board back to Multi-Tech for battery replacement.

Ethernet Ports Caution

The Ethernet ports are not designed to be connected to a Public Telecommunication Network.

Software Recovery CD Warning

Do not use the Software Recovery CD for any purpose except for re-installing software onto the RouteFinder disk drive.

Telecom Warnings for Modem Operation

- Never install telephone wiring during a lightning storm.
- This product must be disconnected from the telephone network interface when servicing.
- This product is to be used with UL and cUL listed computers.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone during an electrical storm. There may be a remote risk of electrical shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- To reduce the risk of fire, use only No. 26 AWG or larger telecommunications line cord.
- Never install telephone jacks in a wet location unless the jack is specifically designed for wet locations.

Safety Recommendations for Rack Installations

- Ensure proper installation of the RouteFinder in a closed or multi-unit enclosure by following the recommended installation as defined by the enclosure manufacturer.
- IMPORTANT: Do not place the RouteFinder directly on top of other equipment or place other equipment directly on top of the RouteFinder.
- If installing the RouteFinder in a closed or multi-unit enclosure, ensure adequate airflow within the rack so that the maximum recommended ambient temperature is not exceeded.
- Ensure that the RouteFinder is properly connected to earth ground via a grounded power cord. If a power strip is used, ensure that the power strip provides adequate grounding of the attached apparatus.
- Ensure that the main supply circuit is capable of handling the load of the RouteFinder. Refer to the power label on the equipment for load requirements.
- Maximum ambient temperature for the RouteFinder is 50 degrees Celsius (120° F).
- This equipment should only be installed by properly qualified service personnel.
- Only connect like circuits. In other words, connect SELV (Secondary Extra Low Voltage) circuits to SELV circuits and TN (Telecommunications Network) circuits to TN circuits.

Shutdown Caution

Never unplug the RouteFinder power until after you have performed the Shutdown process. If the RouteFinder is not properly shut down before unplugging the Power, the next startup may take a little longer, or in the worst case, data could be lost.

Ship Kit Contents

The RouteFinder is shipped with the following:

- One Multi-Tech Systems, Inc. RouteFinder
- One external power supply
- One power cord
- One printed Quick Start Guide
- Two rack mounting brackets and four mounting screws.
- One RouteFinder documentation CD which contains documentation, license agreements, Adobe Acrobat Reader, and license keys.
- A 30-day evaluation copy of VPN client software on CD (not the full working version).
- One RouteFinder Software Recovery CD.

Warning: Do not use the Software Recovery CD for any purpose except for re-installing software onto the RouteFinder hard drive.

Note: If any of these items are missing, contact Multi-Tech Systems or your dealer or distributor. Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the RouteFinder; contact Technical Support at Multi-Tech Systems, Inc. for advice.

License Keys

System License Key

Each RouteFinder ships with a unique individual system License Key, a 20-digit alphanumeric number.

You can view License Key information from the RouteFinder's Web Management software at **Administration > License Key**. This screen shows the entered License Key number and indicates whether it is a valid License Key number.

The License Key number is tied to and tracked with your RouteFinder's serial number. Whenever you require additional licenses, you must first provide Multi-Tech with your current License Key and serial number information in order for us to update your RouteFinder. With a valid License Key, you are entitled to use Multi-Tech's Update service and support.

Note: The system key is already entered into the VPN setup.

URL Categorization License Key

An 11-digit numeric key Universal Resource Locator (URL) Categorization License Key is also shipped with your RouteFinder as part of the 30-day trial offer of the URL software. This Key allows you to set up a URL database that limits clients' access to places on the Internet by blocking sites you do not want accessed. In other words, you can deny users access to various categories of Web sites you select.

What to Do if a Trial License Key Expires

If the license key is a trial key, after expiry of the license period, the WAN interface of the RouteFinder will shut down. If the DHCP client or PPPoE is enabled, they will be disabled. You can connect to the RouteFinder through the LAN interface and enter another valid license key to proceed further. You have to manually enable the DHCP client / PPPoE after entering another valid license key.

AntiVirus License Key

AntiVirus software with its corresponding License Key is available as a special purchase from Multi-Tech.

Where to Find the License Key Number Label

License Key numbers are printed on labels and are located:

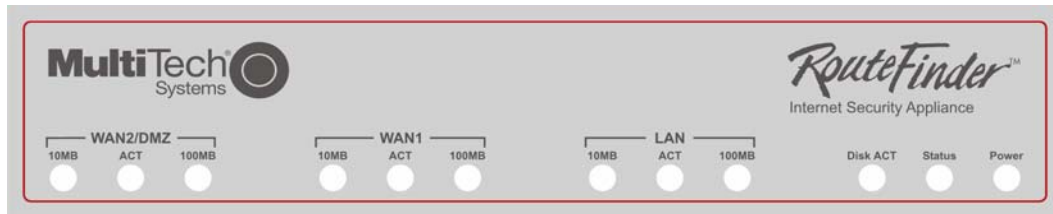
- On the bottom of the RouteFinder chassis
- On the compact flash drive inside the chassis
- On the front cover of the Quick Start Guide.

Chapter 2 – Installation

Installation Notes

See the User Guide for sections on *Planning Your Network* and *Establishing an Address Table*.

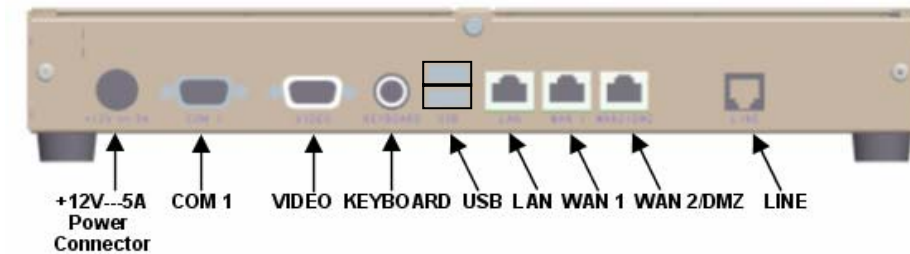
Front Panel



LEDs	Description
10MB	WAN1, WAN2/DMZ: Lights when a successful 10Base-T Internet connection is established. LAN: Lights when a successful 10Base-T Ethernet connection is established.
ACT	WAN1, WAN2/DMZ: Lights when the port has a valid Internet connection. Blinks when it is receiving or transmitting data. LAN: Lights when the LAN port has a valid Ethernet connection. Blinks when it is receiving or transmitting data.
100MB	WAN1, WAN2/DMZ: Lights when a successful 100Base-T Internet connection is established. LAN: Lights when a successful 100Base-T Ethernet connection is established.
Disk ACT	Lights when the disk drive is accessed.
Status	When functioning normally, the LED blinks. The LED is a solid light when the RouteFinder is booting up, saving the configuration, restarting, or updating the firmware.
Power	Lights when power is being supplied to the RouteFinder.

Cabling Procedure

Make the proper connections as illustrated in this drawing of the RouteFinder back panel.



Basic Connections

1. Using an RJ-45 Ethernet cable, connect the **LAN** jack to a PC, internal network switch, or hub.
Note: Use a cross-over Ethernet cable if connecting to a single device.
2. Using an RJ-45 Ethernet cable, connect the **WAN 1** jack to a cable modem or DSL modem connected to an Internet Service Provider.
3. Using the supplied **POWER** cord, plug one end into the RouteFinder power plug, and the other end into a live power outlet.
Note: The status LED blinks continuously after power-up.
4. Wait for the RouteFinder to beep five times, indicating that it is ready to be configured with a Web browser. This may take two or three minutes.

Optional Connections

1. Using an RJ-45 Ethernet cable, connect the **WAN /DMZ** jack to a network or DMZ device. For example, a Voice over IP gateway.
2. Using a DB-9 cable, connect **COM 1** port to a mouse or the COM port on a PC.
3. Using a DB-15 DSUB cable, connect the **VIDEO** port to a monitor.
4. Connect the Keyboard jack to a keyboard.
5. Using a USB connector, connect a memory stick, a floppy drive, a CD-ROM drive, a keyboard, mouse, etc.

Setting up a Workstation and Starting the RouteFinder

This section of the Quick Start covers the steps for setting up TCP/IP communication on the PC(s) connected to the RouteFinder, starting up the RouteFinder, and opening the RouteFinder Web Management program.

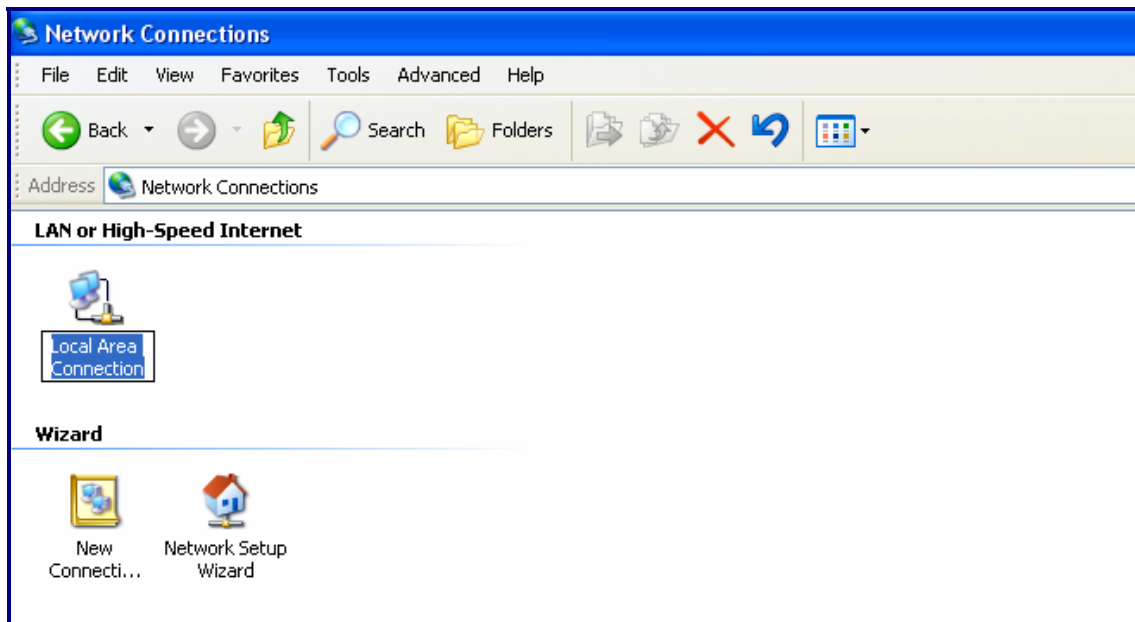
Establish TCP/IP Communication

The RouteFinders have built-in DHCP server functionality, so you can set the PC to obtain a dynamic IP address. The following directions are for Windows 2000+/XP operating systems.

Obtain a Dynamic IP Address

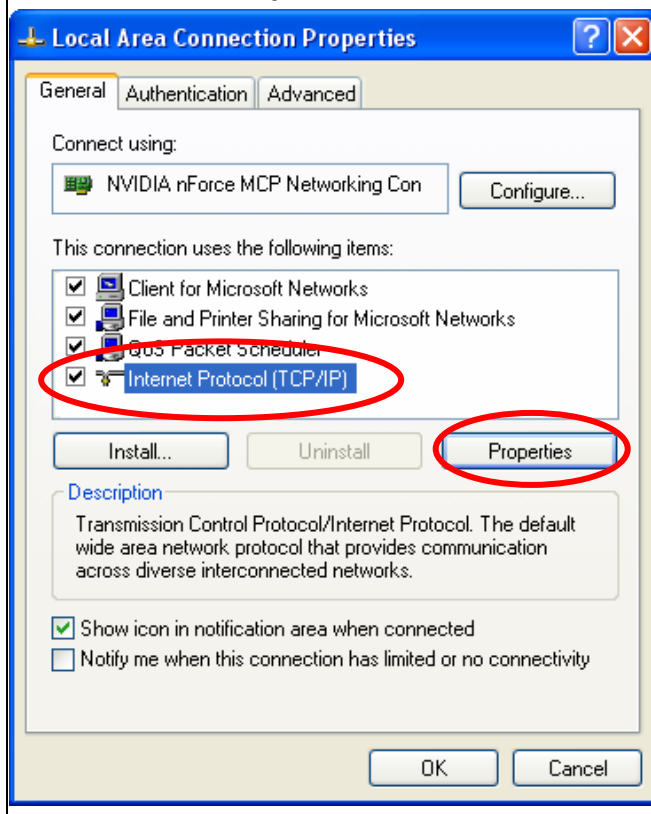
To obtain a dynamic IP address so it can be assigned to the Ethernet port:

1. Make the RouteFinder connections as described on the previous two pages.
2. Click **Start | Settings | Control Panel**. Double-click the **Network Connections** icon.
3. The **Network Connections** screen displays. Right-click the **Local Area Connection** icon and choose **Properties** from the drop down list.

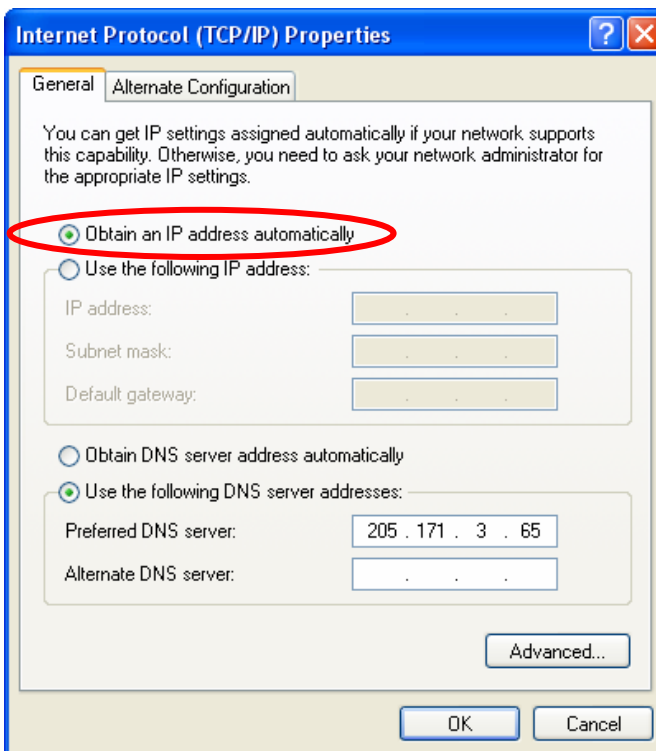


4. The **Local Area Connection Properties** dialog box displays.

- Select **Internet Protocol [TCP/IP]**.
- Click the **Properties** button.



5. Once you click the Properties button, the following screen displays. To have your DHCP client obtain a dynamic IP address, click the button for **Obtain an IP address automatically**.



6. Close out of the Control Panel.
7. Repeat these steps for each PC on your network.

To Set a Fixed IP Address

To set a Fixed IP Address, check **Specify an IP address** instead of **Obtain an IP address automatically**. Then click **OK**.

1. Enter the workstation IP address as **192.168.2.x**. Note that the **x** in the address stands for numbers 101 and up.
2. Enter the Subnet mask as 255.255.255.0
3. Enter the Default gateway as 192.168.2.1
4. Close out of the Control Panel.
5. Repeat these steps for each PC on your network.

Open a Web Browser

Note: Be sure that the RouteFinder is cabled and that the power is connected. See the cabling drawings at the beginning of this chapter.

Bring up a Web browser on the workstation.

- Type the default Gateway address: **https://192.168.2.1**
- Press Enter



IMPORTANT: Be sure to type **https** (**http** will not work).

Note: Make sure your PC's IP address is in the same network as the router's IP address.

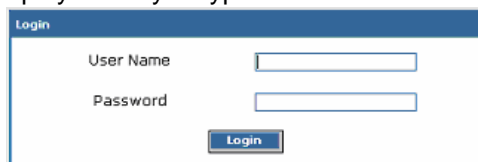
IPCONFIG is a tool for finding a computer's default gateway and MAC address.

In some environments, one or more Security Alert screen(s) may display. At the following **Security Alert** screen, click **Yes** and follow any additional on-screen prompts.



Login

The **Login** screen displays after you type the default Gateway address:

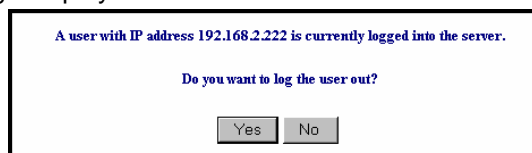


- Type the default User name: **admin** (all lower-case)
- Tab to the Password field and type the default password: **admin** (all lower-case).
- Click the **Login** button.

Note: **User name** and **Password** entries are case-sensitive (both must be typed in lower-case). A password can be up to 12 characters. If Windows displays the **AutoComplete** screen, you may want to click **No** to tell Windows OS to not remember the password for security reasons.

Password Caution: Use a safe password! Your first name spelled backwards is not a sufficiently safe password; a password such as xft35\$4 is better. It is recommended that you change the default password. Create your own password.

- If someone else is already logged into the RouteFinder or you were logged in recently, the following message displays.



Click **Yes**. (If you click **No**, you are returned to the Login screen.)

Web Management Software Opens

The Web Management software Home screen displays.

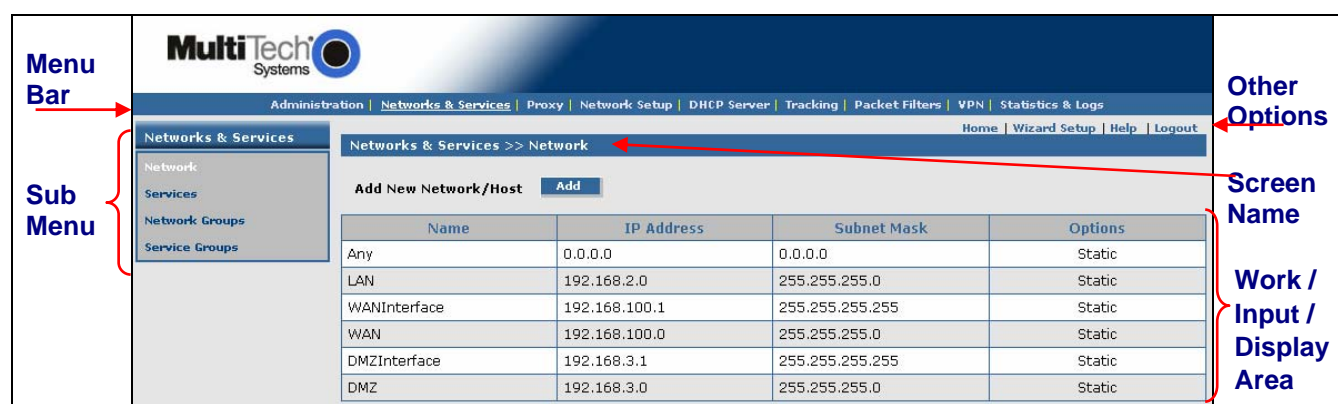
This software is factory-installed on your RouteFinder.

(This is a view of the top part of the Home screen.)



Navigating Through the Software Screens

Before using the software, you may find the following information about navigating the screens and the structuring of the menus helpful.



RouteFinder Menu Bar



Sub-Menu

Each item on the Menu Bar has its own sub-menu, which displays on the left side of the screen.

When you click one of the Menu Bar buttons, the first sub-menu option displays. You can choose other sub-menu screens by clicking the screen name in the sub-menu list.

This is an example of the **Networks & Services** sub-menu.



Other Screen Options

Home	The main screen.
Wizard Setup	Change passwords and quickly set up your RouteFinder with the basic configuration that will set it up as a firewall.
Help	Describes what to do on each screen.
Logout	Logout and return to the login screen.

Menus and Sub-Menus

Administration	Networks & Services	Proxy	Network Setup	DHCP Server
System Setup SSH SNTP Client Administrative Access Change Root Password Site Certificate License Key Intrusion Detection Tools System Scheduler Factory Defaults User Authentication Local Users Radius & SAM Version Information Restart Shutdown	Networks Services Network Groups Service Groups	HTTP Proxy Custom Filters SMTP Proxy SMTP SPAM Filtering POP3 Proxy POP3 SPAM Filtering Advanced Configurations SOCKS Proxy DNS Proxy	Interface PPP PPPoE DHCP Client Dynamic DNS Routes Masquerading SNAT DNAT Load Balancing High Availability	Subnet Settings Fixed Addresses
Tracking	Packet Filters	VPN	Statistics & Logs	
Accounting Update Services Backup Version Control	Packet Filter Rules ICMP Advanced Enable/Disable Log QoS	IPSec X.509 Certificates IPSec Bridging PPTP	Uptime Hardware Networks Interfaces SMTP Proxy Accounting Self Monitor IPSec PPTP Packet Filter Port Scans View Logs HTTP Access DHCP SMTP Virus Quarantine POP3 Virus Quarantine SMTP Spam Quarantine Administrative Authentication Log QoS	

Chapter 3 – Configuration Using Web Management Software

Initial Configuration Step

Set Up Your Time Zone

- Click **Administration** on the Menu Bar. The **System Setup** screen displays.
- Set the following:

Set **System Time** by selecting your **Time Zone**

Set the current **Day, Month, Year, Hour, and Minute**

The screenshot displays the MultiTech Systems web management interface. On the left, a vertical menu bar is labeled **Administration** and **System Setup**. The **Administration** menu is expanded, showing options like System Setup, SSH, SNMP Client, Administrative Access, Change Root Password, Site Certificate, License Key, Intrusion Detection, Tools, System Scheduler, Factory Defaults, User Authentication, Local Users, Radius & SAM, Version Information, Restart, and Shutdown. The **System Setup** screen is displayed, showing the **Administration >> System Setup** page. The **E-Mail Notification** section includes an E-Mail Address field (admin@yourdomain.com) and a **Configure E-Mail Notification** section with a table of events to monitor. The **System Logging** section includes a Logging Status checkbox, Type of Logging (Local/Remote), Remote Syslog Host IP Address, and a Clean Current & Backup Logs button. The **System Time** section includes a Time Zone dropdown (America:Mexico_City), Day, Month, Year, Hour, and Minute dropdowns, and Save buttons.

Administration

System Setup

Submenu and first screen listed on the submenu (*System Setup*) display when you click on your Menu choice (*Administration*)

System Time

MultiTech Systems

Administration | Networks & Services | Proxy | Network Setup | DHCP Server | Tracking | Packet Filters | VPN | Statistics & Logs

Home | Wizard Setup | Help | Logout

Administration >> System Setup

E-Mail Notification

E-Mail Address: **Save** **Delete**

Configure E-Mail Notification:

Don't Send E-Mail Notification for	Action	Send E-Mail Notification for
Export Backup	Add >>	Invalid Web Login
File Intrusion Detected		Invalid SSH Login
High CPU/RAM usage		Virus Key will Expire
Disk Clean Up - Low Diskspace	<< Delete	Virus Key Expired
System Key Expired		URL Filtering Key Expired

System Logging

Logging Status: ☐

Type of Logging: ☒ Local ☐ Remote

Remote Syslog Host IP Address:

Save

Clean Current & Backup Logs: **Clean**

System Time

Time Zone: **Save**

Day: **Save**

Month:

Year:

Hour:

Minute:

Second Configuration Step - Using the Wizard Setup

Using the Wizard Setup is a quick way to enter the basic configuration parameters to allow communication between the LAN's workstation(s) and the Internet as shown in the example below.

The Wizard Setup Screen

Click on the **Wizard Setup** button located under the Menu Bar. The Wizard Setup screen displays. The screen establishes the firewall setup and can be used to enter initial data for other setups.

The Wizard Setup screen is divided into several sections:

- General Settings:**
 - Administrator Mail Address:
 - Hostname:
- LAN Settings:**
 - LAN IP Address:
 - Subnet Mask:
- WAN Settings:**
 - WAN IP Address: ☐ Static IP Address, ☐ PPPoE, ☐ DHCP Client
 - WAN IP Address:
 - Subnet Mask:
 - Gateway:
 - DNS IP Address:
- Modem Settings:**
 - PPP dial backup: ☐
- Password Settings:**
 - root Password:
 - Confirm root Password:
 - Webadmin Password:
 - Confirm Webadmin Password:
 - SSH admin Password:
 - Confirm SSH admin Password:
- Packet Filter rule:**
 - ☒ LAN -- ANY -- ANY -- ACCEPT

At the bottom right, there are **Save** and **Cancel** buttons.

1. Enter your **Administrator Email Address** (can be anything). Example: admin@yourdomain.com
2. Enter your **Hostname** for the RouteFinder (can be anything). Example: RouteFinder.domainname.com
3. **LAN IP Address** and **Subnet Mask** default into the fields. These should be acceptable for your site.
4. Enter the **WAN IP Address**. This is the PUBLIC STATIC IP address. Set this option based on information provided by your ISP. Example: 204.26.122.103
5. Change the **Gateway IP address**. This is the IP address of the router that connects to the Internet. Example: 204.26.122.1
6. Place a checkmark in the **Packet Filter Rule LAN-ANY-ANY-ACCEPT** box to enable the rule.
7. Change **Password Settings** as appropriate for your network. It is highly recommended that you change all default passwords. Do not leave them at the defaults for security reasons.
8. Click **Save** to save the settings you just entered.
9. The following message displays. Click **OK** to close the message box and save your changes.

*Click OK to save the changes. Please be patient.
Setup will take a few minutes to implement the changes.
Do not close the Browser.*

Click **OK** to close the message box and save your changes.

10. One more message displays. Note that saving your settings will take 1-2 minutes.

*Please do not close the browser. Server is saving the values.
After a few minutes you will be redirected to the new IP address.
If you are not redirected, change the address in the location bar to 192.168.2.1.*

11. Test your workstation to see that it can access the Internet. If a connection is established, then the settings have been entered correctly.

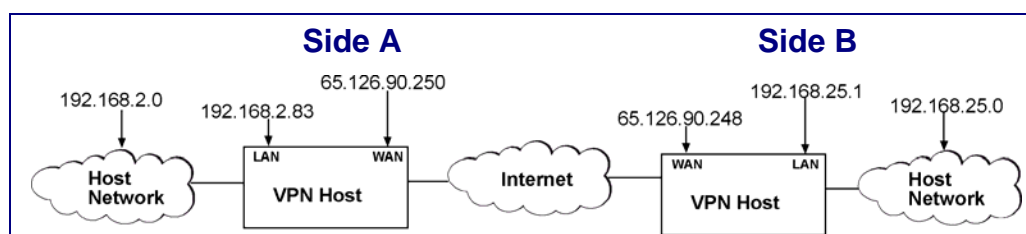
Your Basic Firewall Configuration Is Now Complete.

Chapter 4 – Configuration Examples

These examples show how to configure the RouteFinder using the Web Management software program. The Wizard Setup utility provides a basic firewall connection, while the Web Management software allows you to configure VPN features, management features, and other options.

Example 1 – Setup Two RouteFinders

The example can be used for a LAN-to-LAN (branch office) setup. It requires two RouteFinders - one in the home office and one in the remote branch office and requires additional parameters beyond the Wizard Setup to be entered.



RouteFinder Setup – Side A

Step 1 – Networks & Services > Networks

1. Log in to your RouteFinder software and go to **Networks & Services > Network Configuration** screen.
2. Click the **Add** button to open the fields for entering your network information.
3. Create a new network name for the Remote WAN by entering a **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:
Name: Remote-WAN
IP Address: 65.126.90.248
Subnet Mask: 255.255.255.255
4. Create a new network name for the Remote LAN by entering a **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:
Name: Remote-LAN
IP Address: 192.168.25.0
Subnet Mask: 255.255.255.0
5. Click **Add** to add the network to the list.

Networks & Services >> Network			
Add New Network/Host		<input type="button" value="Add"/>	
Name	IP Address	Subnet Mask	Options
Any	0.0.0.0	0.0.0.0	Static
LAN	192.168.2.0	255.255.255.0	Static
WANInterface	192.168.100.1	255.255.255.255	Static
WAN	192.168.100.0	255.255.255.0	Static
DMZInterface	192.168.3.1	255.255.255.255	Static
DMZ	192.168.3.0	255.255.255.0	Static
Remote-WAN	65.126.90.248	255.255.255.255	Edit Delete
Remote-LAN	192.168.25.0	255.255.255.0	Edit Delete

Step 2 – Packet Filters > Packet Filter Rules

1. Go to the **Packet Filters > Packet Filter Rules** screen to set the VPN client tunnel rights. The Packet Filter rights established on this screen give the client access across the tunnel to your host network.
2. In the *System Defined Rules* section, uncheck the **Status** box, if a check mark is present when setting up *User Defined Rules*.
3. In the *Add User Defined Packet Filter Rules* section, click on **From (Host/Networks)** and select the network to be allowed.
In this example, select **Remote-WAN**.
4. If you are not restricting the type of service, select **Any**.
5. If you are not restricting what network. Click on **To (Host/Network)**, select **Any**.

Notes:

- If the client is dynamic (unknown), set up a **Remote-WAN Any Any ACCEPT** filter to allow any network to come in.
- You might want to add **LAN Any Any ACCEPT** to the *User Defined Packet Filter Rules*. If you want this rule to be in the first position so that it takes precedence over the *VPN-Client* rule, select the **Move** command, and move this rule to the first position.

Packet Filters >> Packet Filter Rules

Show Packet Filter Rules

Show Packet Filter Rules in Popup Window [Show](#)

System Defined Rules

Status	From	Service Group	To	Action	Remarks
<input type="checkbox"/>	LAN/DMZ	default_outbound	WAN	ACCEPT	Allow Outbound Access

Add User Defined Packet Filter Rules

From (Host/Networks): **Any** Service/Service Group: **Any** To (Host/Networks): **Any** Action: **ACCEPT** [Add](#)

No.	From (Host/Networks)	Service/Service Group	To (Host/Networks)	Action	Command
1	LAN	Any	Any	ACCEPT	Edit Delete Move
2	Remote-WAN	Any	Any	ACCEPT	Edit Delete Move
3	Remote-LAN	Any	Any	ACCEPT	Edit Delete Move

Step 3 – VPN Setup

1. Go to the **VPN > IPSec** screen.
2. Click the **VPN Status** check box to enable IPSec. Then click the **Save** button.
3. Select **Add IKE Connection** by clicking the corresponding **Add** button.

VPN >> IPSec

IPSec

VPN Status ☒ [Save](#)

Add New Connection

Add IKE Connection [Add](#)

Add Manual Connection [Add](#)

Status	Connection Name	Local Wan IP	Local LAN	Remote Gateway IP	Remote LAN	Command
--------	-----------------	--------------	-----------	-------------------	------------	---------

Step 3 – VPN Setup (Continued)

The **Add IKE Connection** screen displays. All settings can be left at the default unless otherwise indicated:

1. **Connection Name:** Enter in the name of the VPN tunnel you want to create.
Example: Test-Tunnel
2. **Secret:** Enter a Secret password (which has to match on both ends of the tunnel). For this example, enter **test**.
3. **Select Encryption:** Select **3DES**.
4. **Local WAN IP:** Select **WAN**.
5. **Local LAN:** Select **LAN**.
6. **Remote Gateway IP:** Select **Remote-WAN**. (select **ANY** if unknown)
7. **Remote LAN:** Select **Remote-LAN**.
8. Click the **Save** button to save your tunnel.

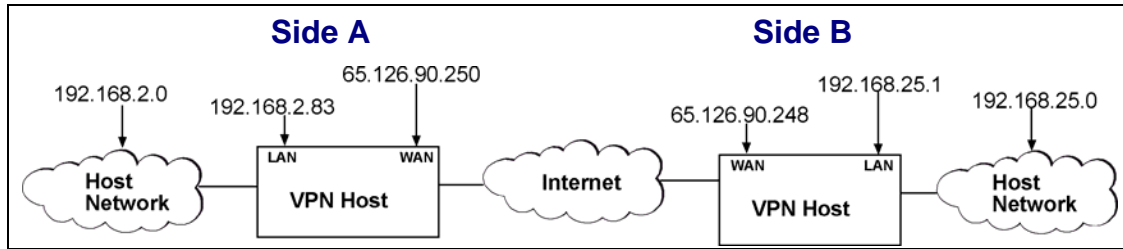
The **VPN > IPSec** Status screen displays; this time showing the newly-created VPN tunnel.

Status	Connection Name	Local Wan IP	Local LAN	Remote Gateway IP	Remote LAN	Command
<input checked="" type="checkbox"/>	Test-Tunnel	WAN	LAN	Remote-WAN	Remote-LAN	Edit Delete

Important Note:

Make sure to check the **Status** box for this VPN tunnel in order to activate it.

RouteFinder Setup – Side B



Step 1 – Networks & Services > Network

1. Log in to your RouteFinder software and go to **Networks & Services > Network Configuration** screen.
2. Click the **Add** button to open the fields for entering your network information.
3. Create a new network name for the Remote LAN by entering a **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:
Name: Remote-LAN
IP Address: 192.168.2.0
Subnet Mask: 255.255.255.0
4. Click **Add** to add the network to the list.
5. Create a new network name for the Remote WAN by entering a **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:
Name: Remote-WAN
IP Address: 65.126.90.250
Subnet Mask: 255.255.255.255
6. Click **Add** to add the network to the list

Note: The same address/mask pair should not be present in the current list displayed on the screen.

Networks & Services >> Network			
Add New Network/Host		<input type="button" value="Add"/>	
Name	IP Address	Subnet Mask	Options
Any	0.0.0.0	0.0.0.0	Static
LAN	192.168.25.0	255.255.255.0	Static
WANInterface	192.168.100.1	255.255.255.255	Static
WAN	192.168.100.0	255.255.255.0	Static
DMZInterface	192.168.3.1	255.255.255.255	Static
DMZ	192.168.3.0	255.255.255.0	Static
Remote-WAN	65.126.90.250	255.255.255.255	Edit Delete
Remote-LAN	192.168.2.0	255.255.255.0	Edit Delete

Step 2 – Packet Filters > Packet Filter Rules

1. Go to the **Packet Filters > Packet Filter Rules** screen to set the VPN client tunnel rights. The Packet Filter rights established on this screen give the client access across the tunnel to your host network.
2. In the *System Defined Rules* section, uncheck the **Status** box, if a check mark is present when adding *User Defined Packet Filter Rules*.
3. In the *Add User Defined Packet Filter Rules* section, click on **From (Host/Networks)** and select the network to be allowed.
In this example, select **Remote-LAN**.
4. If you are not restricting the type of service, select **Any**.
5. If you are not restricting what network. Click on **To (Host/Network)**, select **Any**.

Notes:

- If the client is dynamic (unknown), set up a **Remote-LAN Any Any ACCEPT** filter to allow any network to come in.
- You will need to add **LAN Any Any ACCEPT** to the *User Defined Packet Filter Rules*. If you want this rule to be in the first position so that it takes precedence over the *VPN-Client* rule, select the **Move** command, and move this rule to the first position.

Packet Filters >> Packet Filter Rules

Show Packet Filter Rules

Show Packet Filter Rules in Popup Window Show

System Defined Rules

Status	From	Service Group	To	Action	Remarks
<input type="checkbox"/>	LAN/DMZ	default_outbound	WAN	ACCEPT	Allow Outbound Access

Add User Defined Packet Filter Rules

From (Host/Networks): Any Service/Service Group: Any To (Host/Networks): Any Action: ACCEPT Add

No.	From (Host/Networks)	Service/Service Group	To (Host/Networks)	Action	Command
1	LAN	Any	Any	ACCEPT	Edit Delete Move
2	Remote-WAN	Any	Any	ACCEPT	Edit Delete Move
3	Remote-LAN	Any	Any	ACCEPT	Edit Delete Move

Step 3 – VPN Setup

1. Go to the **VPN > IPSec** screen.
2. Click the **VPN Status** check box to enable IPSec. Then click the **Save** button.
3. Select **Add an IKE Connection** by clicking the corresponding **Add** button.

VPN >> IPSec

IPSec

VPN Status ☒ Save

Add New Connection

Add IKE Connection Add

Add Manual Connection Add

Status	Connection Name	Local Wan IP	Local LAN	Remote Gateway IP	Remote LAN	Command
--------	-----------------	--------------	-----------	-------------------	------------	---------

Step 3 – VPN Setup (Continued)

The **Add an IKE Connection** screen displays. All settings can be left at the default unless otherwise indicated:

1. **Connection Name:** Enter in the name of the VPN tunnel you want to create. Example: Test-Tunnel.
2. **Secret:** Enter the **Secret** password (which has to match on both ends of the tunnel). For this example, enter **test**.
3. **Select Encryption:** Select **3DES**.
4. **Local WAN IP:** Select **WAN**
5. **Local LAN:** Select **LAN**
6. **Remote Gateway IP:** Select **Remote-WAN** (Select **Any** if unknown)
7. **Remote LAN:** Select **Remote-LAN**.
8. Click the **Save** button to save your tunnel.

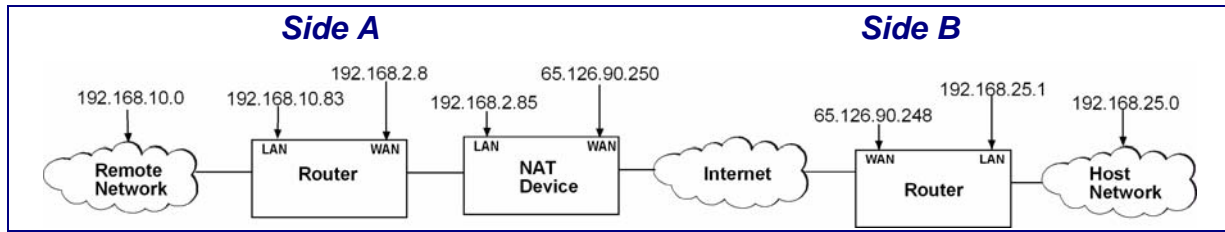
The **VPN > IPSec** Status screen displays; this time showing the newly-created VPN tunnel.

Status	Connection Name	Local Wan IP	Local LAN	Remote Gateway IP	Remote LAN	Command
<input checked="" type="checkbox"/>	Test-Tunnel	WAN	LAN	Remote-WAN	Remote-LAN	Edit Delete

Important Note:

Make sure to check the **Status** box for this VPN tunnel in order to activate it.

Example 2 – Set Up Two RouteFinders Behind a NAT Device



RouteFinder Setup – Side A

Step 1 – Networks & Services > Networks

1. Login to your RouteFinder and go to the **Networks & Services > Network Configuration** screen.
2. Click the **Add** button to open the fields for entering the network information.
3. Create a new network name for the RF850-LAN by entering the **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:
Name: RF850-LAN
IP Address: 192.168.25.0
Subnet Mask: 255.255.255.0
4. Click the **Add** button to add the new network to the list.
5. Create a new network name for the RF850-WAN by entering the **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:
Name: RF850-LAN
IP Address: 65.126.90.248
Subnet Mask: 255.255.255.255
6. Click the **Add** button to add the new network to the list.

Networks & Services >> Network			
Add New Network/Host		<input type="button" value="Add"/>	
Name	IP Address	Subnet Mask	Options
Any	0.0.0.0	0.0.0.0	Static
LAN	192.168.10.0	255.255.255.0	Static
WANInterface	192.168.2.8	255.255.255.255	Static
WAN	192.168.2.0	255.255.255.0	Static
DMZInterface	192.168.3.1	255.255.255.255	Static
DMZ	192.168.3.0	255.255.255.0	Static
RF850-LAN	192.168.25.0	255.255.255.0	Edit Delete
RF850-WAN	65.126.90.248	255.255.255.255	Edit Delete

Step 2 – Packet Filters > Packet Filter Rules

1. Go to the **Packet Filters > Packet Filters Rules** screen to set the VPN client tunnel rights. The Packet Filter rights established on this screen give the client access across the tunnel to your host network.
2. In the *System Defined Rules* section, uncheck the **Status** box, if a check mark is present.
3. In the *Add User Defined Packet Filter Rules* section, click on **From (Host/Networks)** and select the network to be allowed.
In this example, select **RF850-LAN**.
4. If you are not restricting the type of service, select **Any**.
5. If you are not restricting what network. Click on **To (Host/Network)**, select **Any**.

Notes:

- If the client is dynamic (unknown), set up an **RF850-LAN Any Any ACCEPT** filter to allow any network to come in.
- You might want to add **LAN Any Any ACCEPT** to the *User Defined Packet Filter Rules*. If you want this rule to be in the first position so that it takes precedence over the *VPN-Client* rule, select the **Move** command, and move this rule to the first position.

Packet Filters >> Packet Filter Rules

Show Packet Filter Rules

Show Packet Filter Rules in Popup Window Show

System Defined Rules

Status	From	Service Group	To	Action	Remarks
<input type="checkbox"/>	LAN/DMZ	default_outbound	WAN	ACCEPT	Allow Outbound Access

Add User Defined Packet Filter Rules

From (Host/Networks): **Any** Service/Service Group: **Any** To (Host/Networks): **Any** Action: **ACCEPT** Add

No.	From (Host/Networks)	Service/Service Group	To (Host/Networks)	Action	Command
1	LAN	Any	Any	ACCEPT	Edit Delete Move
2	RF850-LAN	Any	Any	ACCEPT	Edit Delete Move
3	RF850-WAN	Any	Any	ACCEPT	Edit Delete Move

Step 3 – VPN Setup

1. Go to the **VPN > IPSec** screen.
2. Click on the **VPN Status** check box to enable IPSec. Then click the **Save** button.
3. Select **Add an IKE Connection** by clicking the corresponding **Add** button.

VPN >> IPSec

IPSec

VPN Status ☒ Save

Add New Connection

Add IKE Connection Add

Add Manual Connection Add

Status	Connection Name	Local Wan IP	Local LAN	Remote Gateway IP	Remote LAN	Command
--------	-----------------	--------------	-----------	-------------------	------------	---------

Step 3 – VPN Setup (Continued)

The **Add IKE Connection** screen displays. All settings can be left at the default unless otherwise indicated:

1. **Connection Name:** Enter a name for the VPN tunnel you want to create. For this example, enter **Behind-NAT**.
2. **Secret:** Enter the **Secret** password (which has to match on both ends of the tunnel). For this example, enter **test**.
3. **Select Encryption:** Select **3DES**.
4. **Local WAN IP:** Select **WAN**.
5. **Local LAN:** Select **LAN**.
6. **Remote Gateway IP:** Select **RF850-WAN**.
7. **Remote LAN:** Select **RF850-LAN**.
8. **UID:** Click the **Enable** button (must be enabled when using NAT).
9. **Local ID:** Enter the local security gateway ID (required when using NAT). For this example, enter 192.168.2.8
10. **Remote ID:** Enter the remote security gateway ID (required when using NAT). For this example, enter 65.126.90.248
11. Click the **Add** button to save your tunnel.

The **VPN > IPSec** Status screen displays; this time showing the newly-created VPN tunnel.

Important Note:
 Make sure to check the **Status** box for this VPN tunnel in order to activate it.

VPN >> IPSec

IPSec

VPN Status ☒ **Save**

Add New Connection

Add IKE Connection **Add**

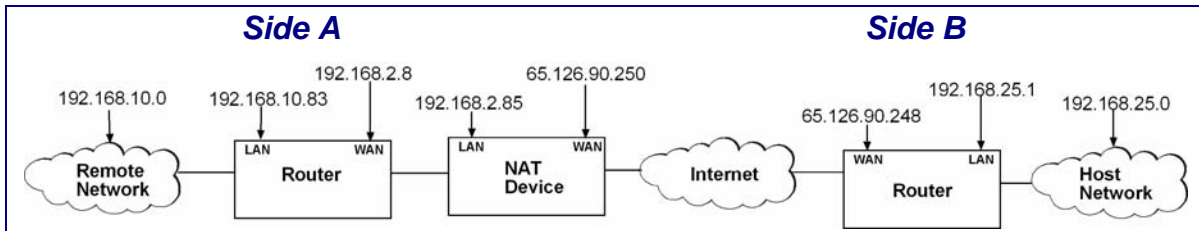
Add Manual Connection **Add**

Status	Connection Name	Local Wan IP	Local LAN	Remote Gateway IP	Remote LAN	Command
<input checked="" type="checkbox"/>	Behind-NAT	WAN	LAN	RF850-WAN	RF850-LAN	Edit Delete

Multi-Tech Systems, Inc. RouteFinder RF850/860 Quick Start Guide (82100051L)

23

RouteFinder Setup – Side B



Step 1 -- Network & Services > Network

1. Log into your RouteFinder and go to the **Networks & Services > Network Configuration** screen.
2. Click the **Add** button to open the fields for entering your network information.
3. Create a new network name for the RF850-WAN by entering the **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:
Name: RF850-WAN
IP Address: 65.126.90.250
Subnet Mask: 255.255.255.255
4. Click the **Add** button to add the new network to the list.
5. Create a new network name for the RF850-LAN by entering the **Name**, **IP Address**, and **Subnet Mask**. For this example, enter the following:
Name: RF850-LAN
IP Address: 192.168.10.0
Subnet Mask: 255.255.255.0
6. Click the **Add** button to add the new network to the list.

Networks & Services >> Network			
Add New Network/Host		<input type="button" value="Add"/>	
Name	IP Address	Subnet Mask	Options
Any	0.0.0.0	0.0.0.0	Static
LAN	192.168.25.0	255.255.255.0	Static
WANInterface	65.126.90.248	255.255.255.255	Static
WAN	65.126.90.0	255.255.255.0	Static
DMZInterface	192.168.3.1	255.255.255.255	Static
DMZ	192.168.3.0	255.255.255.0	Static
RF850-LAN	192.168.10.0	255.255.255.0	Edit Delete
RF850-WAN	65.126.90.250	255.255.255.255	Edit Delete

Step 2 – Packet Filters > Packet Filter Rules

1. Go to the **Packet Filters > Packet Filter Rules** screen to set the VPN client tunnel rights. The Packet Filter rights established on this screen give the client access across the tunnel to your host network.
2. In the *System Defined Rules* section, uncheck the **Status** box, if a check mark is present.
3. In the *Add User Defined Packet Filter Rules* section, click on **From (Host/Networks)** and select the network to be allowed. In this example, select **RF850-WAN**.
4. If you are not restricting the type of service, select **Any**.
5. If you are not restricting what network. Click on **To (Host/Network)**, select **Any**.

Notes:

- If the client is dynamic (unknown), set up an **RF850-WAN Any Any ACCEPT** filter to allow any network to come in.
- You might want to add **LAN Any Any ACCEPT** to the *User Defined Packet Filter Rules*. If you want this rule to be in the first position so that it takes precedence over the *VPN-Client* rule, select the **Move** command, and move this rule to the first position.

Packet Filters >> Packet Filter Rules

Show Packet Filter Rules

Show Packet Filter Rules in Popup Window Show

System Defined Rules

Status	From	Service Group	To	Action	Remarks
<input type="checkbox"/>	LAN/DMZ	default_outbound	WAN	ACCEPT	Allow Outbound Access

Add User Defined Packet Filter Rules

From (Host/Networks) Any Service/Service Group Any To (Host/Networks) Any Action ACCEPT Add

No.	From (Host/Networks)	Service/Service Group	To (Host/Networks)	Action	Command
1	LAN	Any	Any	ACCEPT	<a>Edit <a>Delete <a>Move
2	RF850-LAN	Any	Any	ACCEPT	<a>Edit <a>Delete <a>Move
3	RF850-WAN	Any	Any	ACCEPT	<a>Edit <a>Delete <a>Move

Step 3 -- VPN Setup

1. Go to the **VPN > IPSec** screen.
2. Click on the **VPN Status** check box to enable IPSec. Then click the **Save** button.
3. Select **Add an IKE Connection** by clicking the corresponding **Add** button.

VPN >> IPSec

IPSec

VPN Status ☒ Save

Add New Connection

Add IKE Connection Add

Add Manual Connection Add

Status	Connection Name	Local Wan IP	Local LAN	Remote Gateway IP	Remote LAN	Command
--------	-----------------	--------------	-----------	-------------------	------------	---------

Step 3 – VPN Setup (Continued)

The **Add IKE Connection** screen displays. All settings can be left at the default unless otherwise indicated:

1. **Connection Name:** Enter the name of the VPN tunnel you want to create. For this example, enter **Behind-NAT**.
2. **Secret:** Enter the **Secret** password (which has to match on both ends of the tunnel). For this example, enter **test**.
3. **Select Encryption:** Select **3DES**.
4. **Local WAN IP:** Select **WAN**.
5. **Local LAN:** Select **LAN**.
6. **Remote Gateway IP:** Select **RF850-WAN**.
7. **Remote LAN:** Select **RF850-LAN**.
8. **UID:** Click the **Enable** button (must be enabled when using NAT).
9. **Local ID:** Enter the local security gateway ID (required when using NAT). For this example, enter 65.126.90.248
10. **Remote ID:** Enter the remote security gateway ID (required when using NAT). For this example, enter 192.168.2.8
11. Click the **Save** button to save your tunnel.

The **VPN > IPSec** Status screen displays; this time showing the newly-created VPN tunnel.

Important Note:

Make sure to check the **Status** box for this VPN tunnel in order to activate it.

te:

check

x for

el in

te it.

VPN >> IPSec

IPSec

VPN Status ☒ Save

Add New Connection

Add IKE Connection Add

Add Manual Connection Add

Status	Connection Name	Local Wan IP	Local LAN	Remote Gateway IP	Remote LAN	Command
<input checked="" type="checkbox"/>	Behind-NAT	WAN	LAN	RF850-WAN	RF850-LAN	Edit Delete

Example 3 – Remote Client-to-LAN Configuration Using DNAT and Aliasing

Use this procedure to configure the RouteFinder with DNAT and Aliasing. This configuration allows a Windows Remote Client to Telnet through the RouteFinder to several Windows Operating Systems located on the LAN.

Remote Client-to-LAN Configuration Using DNAT and Aliasing Through the RouteFinder

1. Networks & Services > Network screen

Enter: LAN Network, 192.168.2.0, 255.255.255.0
 Enter WANInterface1, 204.26.122.103, 255.255.255.255
 Enter WANInterface2, 210.26.122.104, 255.255.255.255
 Enter WIN2k_Pro, 192.168.2.100, 255.255.255.255
 Enter WIN2k_Server, 192.168.2.11, 255.255.255.255

2. Network Setup > Interface screen

Set default gateway at 204.26.122.1
 Enter a host name (example: RF860.Site-A.com)
 Enter Network Cards: (Cards 1 & 3 are defaulted)
 Card 1: LAN (eth0), 192.168.2.1, 255.255.255.0
 Card 2: WAN (eth1), 204.26.122.103, 255.255.255.0
 Card 3: DMZ (eth2), 192.168.3.1 (this is a default)

3. Network Setup > Interface (IP Aliases section) screen

Interface: Select LAN(eth0)
 Enter IP Address: 204.26.122.104
 Enter Net Mask: 255.255.255.255
 Interface: Select: Select WAN (eth1)
 Enter IP Address: 204.26.122.105
 Enter Net Mask: 255.255.255.255

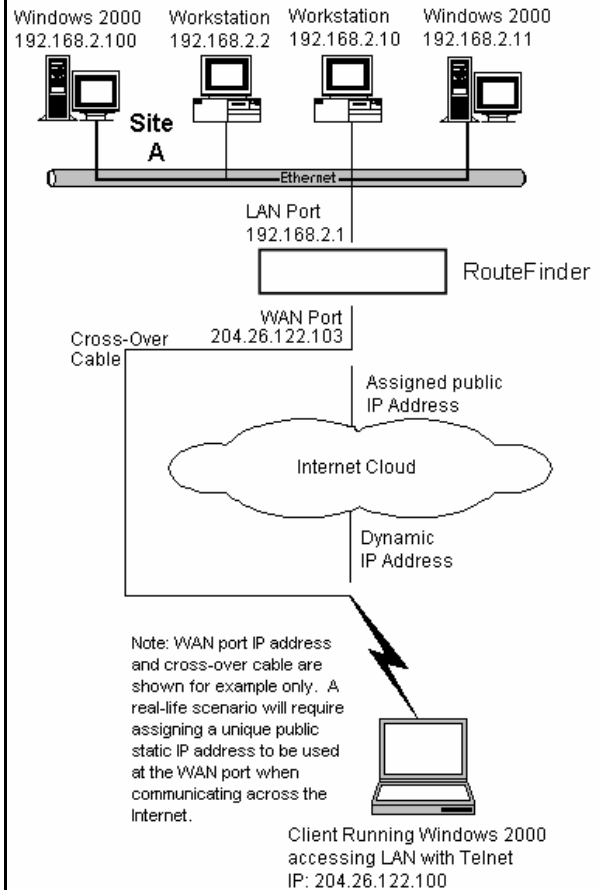
4. Network Setup > DNAT screen

Enter two profiles:

Pre DNAT Network: Select WANInterface1
 Pre DNAT Service: Select Telnet
 Post DNAT IP Address: Select Win2k_Pro
 Post DNAT Service: Select Telnet
 Pre DNAT Network: Select WANInterface2
 Pre DNAT Service: Select Telnet
 Post DNAT IP Address: Select Win2k_Server
 Post DNAT Service: Select Telnet

5. Packet Filters > Packet Filter Rules screen

Add User Defined Packet Filter Rules
 LAN – ANY – ANY – Accept
 ANY – Telnet – Win2k_Pro – Accept
 ANY – Telnet – Win2k_Server – Accept



Example 4 – Client-to-LAN Configuration Using PPTP Tunneling

Use this procedure to configure the RouteFinder as a PPTP server for VPN Remote Client Access. This is also known as the PPTP Roadwarrior configuration.

Note: IPX and Netbeui are not supported when using PPTP tunneling.

Remote Client-to-LAN Configuration Using PPTP Tunneling Through the RouteFinder

1. Networks & Services > Network screen

Enter: LAN Network, 192.168.2.0, 255.255.255.0
Enter: PPTP-Pool, 192.168.2.240, 255.255.255.240

2. Network Setup > Interface screen

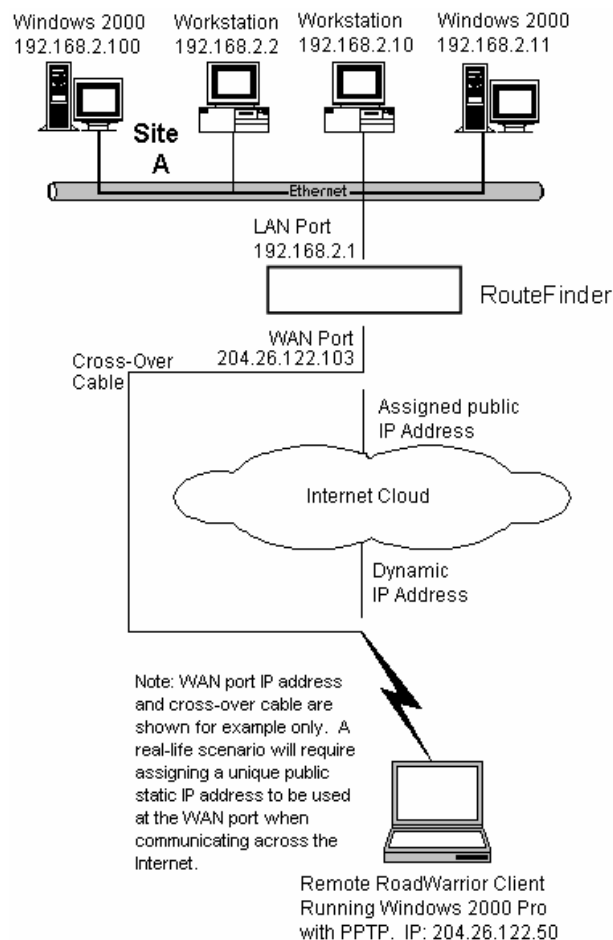
Set default gateway at 204.26.122.1
Enter a host name (example: RF860.Site-A.com)
Enter Network Cards: (Cards 1 & 3 are defaulted)
Card 1: LAN (eth0), 192.168.2.1, 255.255.255.0
Card 2: WAN (eth1), 204.26.122.103, 255.255.255.0
Card 3: DMZ (eth2), 192.168.3.1 (this is a default)

3. Packet Filters > Packet Filter Rules screen

Add User Defined Packet Filter Rules
LAN – ANY – ANY – Accept

4. VPN > PPTP screen

Check the *PPTP Status* box
Encryption Strength: Select *40* or *128*
Select Remote Address: Select *PPTP-Pool*
Click **Save** button. The addresses and range display.
Authentication Type: Select *Local*
Username: Enter user name (example: roadwarrior)
Password: Enter user password (example:1o2t3t4t)
Click the **Add** button.



Checking the Tunnel

After setting up your RouteFinder, you can check the status of your VPN tunnel by clicking on **Statistics & Logs** and going to the **IPSec Live Log**. You will see the connection up and running (if connected), and you will see the statistics related to the data being sent across the tunnel.

Chapter 5 – URL Categorization

The Universal Resource Locator (URL) Categorization License Key allows you to set up a URL database that limits clients' access to places on the Internet by blocking sites you do not want accessed. In other words, you can deny users access to various categories of Web sites you select.

Important Settings

The RouteFinder must be connected to the Internet for the URL License to be activated.

Setting Up HTTP Proxy and URL Filtering

1. Click **Proxy** from the Menu bar. The **HTTP Proxy** screen displays.
2. Check the **Status** box and click **Save**.

Important: **Status** must be checked before you can enter and activate your URL Categorization License Key.

MultiTech Systems

Administration | Networks & Services | **Proxy** | Network Setup | DHCP Server | Tracking | Packet Filters | VPN | Statistics & Logs

Home | Wizard Setup | Help | Logout

Proxy

HTTP Proxy

Custom Filters

SMTP Proxy

SMTP SPAM Filtering

POP3 Proxy

POP3 SPAM Filtering

Advanced Configurations

SOCKS Proxy

DNS Proxy

Proxy >> HTTP Proxy

HTTP Proxy

Status ☒ **Save**

Networks (allowed / denied) **Edit**

Banner Filter ☐ **Save**

Java Script Filter ☐ **Save**

Cookie Filter ☐ **Save**

URL Categorization

URL Filter ☒ **Save**

URL Categories (allowed / filtered) **Edit**

Networks / Hosts to bypass URL Filtering **Edit**

Authentication

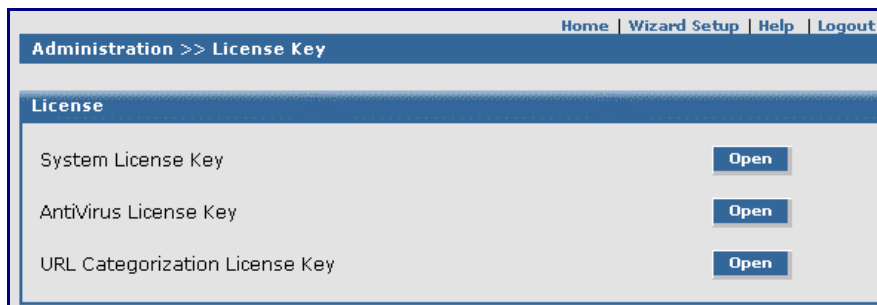
User Authentication ☒ **Save**

Authentication Types **local** **Save**

Available Users	Action	Allowed Users
admin	Add >>	
loginuser	<< Delete	

Note About URL License Key: The URL License number must be entered on the **Administration > License Key** screen before the URL Categorization section of this screen displays. The 30-day free trial key number is located on the bottom of the RouteFinder chassis and on the front of the Quick Start Guide.

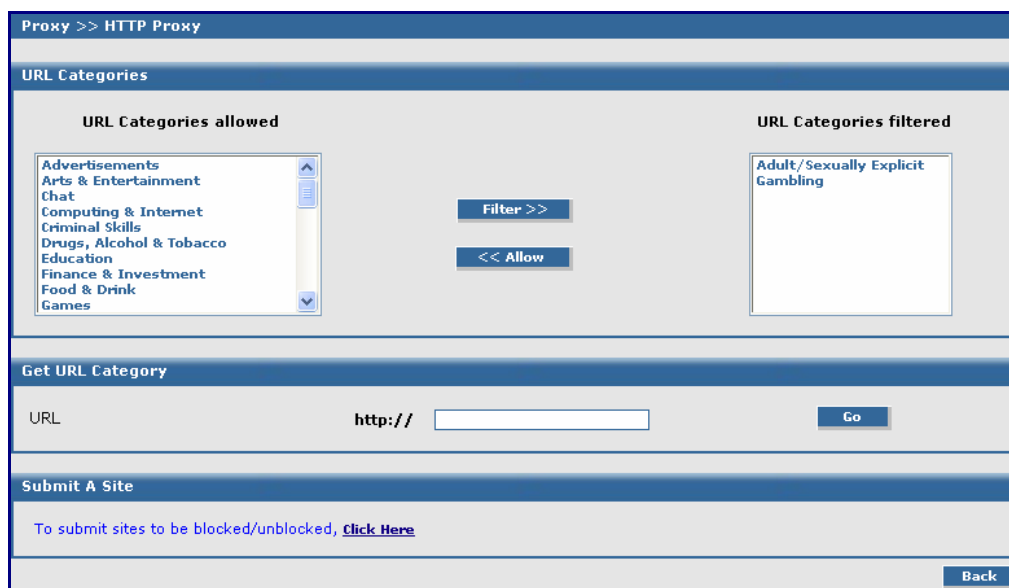
3. Navigate to the **Administration > License Key** screen.
 - For the *URL Categorization License Key*, click the **Open** button.



You can enter a license key; or if the key was already entered, the screen shows the license number and its expiration date. (Screen not shown).

IMPORTANT: It is important that the serial number be entered in upper case. Using upper case letters, enter the 11-digit serial number of the URL License Key and click the **Save** button.

4. Return to the **Proxy > HTTP Proxy** screen. (See the screen on the previous page)
 - Check the **URL Filter** box and click **Save** if not previously checked.
 - Check the **URL Categories (Allowed/Filtered)** box and click **Edit**.
5. The **URL Categories** screen displays. You can use this screen to allow or block Web sites from users.



- Use the **Allow** and **Filter** buttons to move a URL Category from the *URL Categories Allowed* list to the *URL Categories Filtered* or from *Filtered* to *Allowed*.
- When you are finished organizing the categories, click the **Back** button to exit the screen.

How to Test Web Sites for Blocking

You can test specific Web sites to see if the URL has been blocked (use **Get URL Category** to perform this test) or submit a site to be blocked or unblocked by the SurfControl software, which sets up the categories stored in this software.

How to Test the Filtering

Type a URL in the **http://** box and click the **Go** button. This will test the URL to see if it is allowed or blocked.

Note: You can also test a site through your browser by entering a Web address that you feel should be blocked by the filter through one of the categories you had chosen or a category preset by the URL software. For instance, if you selected the **Finance and Investment** category to be filtered, try to access www.etrade.com. This site should be blocked. A message displays under the URL address stating the status of this Web site.

Important: The sites listed in the **Favorites** box of the browser will not be blocked unless the cache is emptied in the browser.

Establishing Filtering Rules for Networks and Hosts

Return to the **Proxy > HTTP Proxy** screen by clicking the **Back** button on the **Proxy > HTTP Proxy > URL Categorization** screen.

- Click the **Edit** button for **Networks / Hosts to bypass URL Filtering**. The **Networks / Hosts to bypass URL Filtering** screen displays. You can use this screen to allow or block Web sites from Networks / Hosts.
- Click the **Add** button to move a network/host name into the **Network/Hosts to Bypass URL Filtering** box.
- If you decide you do not want one or more of the networks/hosts bypassing the filter, select the name and click the **Delete** button. The name moves back into the **Available Networks/Host** box.

Submitting a Site to SurfControl for Reconsideration

Filter categories are setup and controlled by the SurfControl software that is built into your RouteFinder. There may be a category you would like to see added or deleted. The User Guide provides instructions for these requests.

